DEPARTMENT OF THE NAVY
U.S. NAVY PERSONNEL SUPPORT ACTIVITY
DETACHMENT, GUAM
PSC 455, BOX 172
FPO AP 96540-1728

MASTER FILE COPY

PSDGUAMINST 3070.1B
Code 10
14 Jan 99

PERSUPPDET GUAM INSTRUCTION 3070.1B

Subj: OPERATIONS SECURITY (OPSEC) PROGRAM

Ref: (a) OPNAVINST 3070.1A

Encl: (1) Security Indoctrination Briefing, PSAFE Form 5510/1 (Rev. 2-98)

1. Purpose. To establish an Operations Security (OPSEC) Program and delineate management guidelines per reference (a).

2. Cancellation. PERSUPPDETGUAMINST 3070.1A.

3. Background. Operations Security addresses the overall protection of exploitable information, both classified and unclassified. The principal focus of this instruction is to anticipate exploitable information, deny access to foreign collection efforts and eliminate OPSEC vulnerabilities within the command.

4. Action. Per reference (a) and with the goal of increasing OPSEC awareness and the protection of essential secrecy at all times, the following operational guidelines are established:

a. The Security Manager is responsible for the overall command enforcement of OPSEC policies and regulations.

b. The Security Manager shall provide a briefing to all incoming personnel utilizing enclosure (1). Annual training will also be incorporated into the Detachment's General Military Training plan.

5. Conclusion. An effective OPSEC program is an efficient countermeasure to foreign intelligence collection efforts. Operations Security is especially important when operating in an overseas environment and is an all hands responsibility.

F. S. BALTAZAR, JR.

Distribution: PSDGUAMINST 5216.1P
List I (Case B)

Copy to:
PSAFE

SECURITY INDOCTRINATION BRIEFING

AFTER READING EACH PARAGRAPH, INITIAL IN THE SPACE PROVIDED TO ACKNOWLEDGE UNDERSTANDING

_____ 1. Your assignment to the PERSUPPACT Far East network carries with it the responsibility for safeguarding classified information that you may have access to during your assignment at this activity. You are also responsible for helping maintain the security of this activity by complying with the various security regulations issued to provide the necessary measures to guard against any classified information falling into unauthorized hands and to prevent sabotage.

_____ 2. You have been granted access to classified information. You have been evaluated and determined to be worthy of this trust. Now, as a member of the team, you must do your part if the team is to win; and this team must win because it has the responsibility of protecting our national security information.

_____ 3. Now here are some rules. The determination made on information requiring protection is called "classification." There are three levels of national security information which are identified and marked with a classification. These classifications, in order from highest to lowest, are: TOP SECRET, SECRET, and CONFIDENTIAL. Each classification requires specific protective measures. The loss of any classified material will result in damage to national security. Information becomes classified when the official who originates it decides that the information requires protection for reasons of national security.

_____ 4. To assist users of classified documents, the subject and paragraphs are marked with individual classifications so that unclassified material, or material with a lower classification than the overall document, may be used accordingly. The overall document must always be marked with the highest classification or material contained.

_____ 5. Classified documents must always be marked for downgrading and declassification so they can be given a lower classification and declassified as soon as possible. A vigorous program is underway within the Department of Defense to ensure that information requiring security protection is classified at the lowest appropriate level and that it is downgraded *(classification lowered)* and declassified *(classification removed)* at the earliest date. Only when information is classified in this manner will the system work, enabling the public to be given information to which it is entitled, and enabling the Department of Defense to protect information that truly requires safeguarding in the interest of national security. You can assist by calling cases of over/under classification to the attention of your supervisor or the Security/Assistant Security Officer or Manager.

_____ 6. Only give classified information to personnel who have been authorized access to it. There are different levels of personnel security clearances; individuals are cleared for access only to the level of information required for their jobs. For example, personnel whose job requires them to have access to some Secret material will be given a Secret Clearance and may have access to Secret and Confidential information but not Top Secret. However, just because you hold a Secret Clearance does not mean that you have access to all Secret information. You must also have a "need to know," that is, aside from having the proper clearance, your official duties must require you to have the information.

_____ 7. Never leave classified information unprotected. It must be properly stored or left in the custody of a cleared person. During working hours, classified material on desks and in routing baskets should be placed face-down when not in use. During lunch/coffee breaks, classified material must either be locked up or under continuous observation by a cleared individual. Never use locked desk drawers or briefcases to safeguard classified material, not even temporarily. When locking material in safes, spin tumbler locks at least four times and pull drawer handles to ensure the container has been locked.

_____ 8. Do not read or discuss classified information in a non-secure area. Classified information is not to be used where uncleared persons or those without a "need to know" might see or hear it. Friends, family members, and uncleared persons are not permitted to receive or discuss classified information. It is your responsibility to impress upon your family members the importance of properly safeguarding any classified information which may be carelessly or inadvertently revealed to them.

_____ 9. Do not give classified information to a visitor without first certifying his/her identification, clearance, and need to know. Do not ask a messenger to pick-up or deliver classified material without first verifying his/her clearance. No person having knowledge, possession, or control of classified material has the authority to disseminate it, unless he/she has determined that the prospective recipient has an appropriate security clearance and needs the information in order to perform official duties. The responsibility for making these determinations rests upon the person having knowledge, possession, or control of the information, not upon the prospective recipient.

_____ 10. You may not remove classified information from the command except in approved situations and with the specific permission of the CO/OIC as appropriate; if removal of classified material is required in the performance of your duty, official authorization is required. If travel is involved, official travel orders must be issued including a statement authorizing the transport of classified material.

_____ 11. Never discuss classified information over the telephone. This is especially important because a high proportion of DOD phone conversions are being transmitted through microwave transmitters; such conversions can be easily and surreptitiously recorded and analyzed. Types of situations to avoid when talking over the phone are:

a. Allowing classified information to slip into conversation through carelessness *(i.e. ship's movements).*

b. Disclosing classified information to expedite the completion of a "rush project."

c. Using codes, "double talk," or attempting to talk around classified information. *(Private codes and talking around classified information presents no real protection against the abilities of trained analysts.)*

Encl (1)

_____ 12. You may only send classified material out of the command by approved methods. Chapter 12 of OPNAVINST 5510.1 outlines the approved methods of transmission and transportation.

_____ 13. Only dispose of classified material by approved methods and with the required records. Chapter 13 of OPNAVINST 5510.1 outlines approved methods of destruction and records that must be maintained. Preliminary drafts, carbon sheets, stencils, worksheets, and all similar items containing information will be either;

a. Destroyed by the person responsible for their preparation immediately after they have served their purpose; or,

b. Given the same classification and safeguarded in the same manner as the classified material produced from them *(i.e. typewriter ribbons used in typing classified material)*.

_____ 14. Classified information is not personal property and will be returned to the OIC or Department Head when employment is terminated.

_____ 15. Never store security container combinations in non-secure places *(i.e. wallets, under desk blotters, address list finders, etc.)*. Additionally, in selecting combination numbers, avoid using multiples of 5, simple ascending or descending arithmetical series, or personal data such as birthdates. The safe information will not be used for more than one container in any one office.

_____ 16. Whenever an infraction of security regulations comes to your attention, it is your responsibility to report it to your superiors or to the Security Manager. You must promptly report any of the following types of information:

a. Attempts by representatives or citizens of foreign *(particularly communist-controlled)* governments to:

(1) Cultivate a friendship to the extent of placing you under obligation, that you would not normally be able to reciprocate, or to obtain information of intelligence value by money payments or bribery.

(2) Obtain information of intelligence value through observation, collection of documents, or personal contact;

(3) Coerce or blackmail, threats against or promises of assistance to relatives living under foreign control, especially living in a communist country;

(4) Appeal to you on a racial, nationalistic, or ideological basis;

(5) Exploit you or others who may be dissatisfied or in personal difficulties;

(6) Intimidate, harass, entrap, discredit, search, spy on, or recruit you for intelligence purposes; or

(7) Induce you to defect or induce those who have fled from communist countries to re-defect.

b. Attempts by Department of the Navy personnel to provide unauthorized service information or documents to anyone believed to be in contact with a foreign intelligence service.

c. Attempts by persons living in communist countries to obtain information of intelligence value by correspondence, including "Pen Pal" correspondents, questionnaires, "ham radio" activity, Naval Cachets *(requests to service postal covers)*, or other forms of communications.

_____ 17. I have read and fully understand the principles, criteria, and procedures for classification, downgrading, and declassification, including marking of information as prescribed in Chapters 5 through 8 of OPNAVINST 5510.1.

I understand the information and requirements of this Security Briefing.

_____
Signature/Date

I certify that the Security Briefing has been completed.

_____
Signature of Security Manager/Date

PSAFE 5510/1 (Rev. 2-98) (REVERSE)